UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,719	03/08/2001	Eli Yanovsky	00/21252	5130

7590 12/08/2006

Martin D. Moynihan
PRTSI, Inc.
P.O. Box 16446
Arlington, VA 22215

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/800,719	YANOVSKY, ELI	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 13-16, and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Jung et al. ("Encryption with Statistical Self-Synchronization in Synchronous Broadband Networks") in view of Shefi (6,266,413), and further in view of Maurer (5253294).

In reference to claims 1, 13-14, and 21, Jung teaches encryption in the CFB-mode is achieved by XOR-ing the plaintext with the output of a key stream generator (page 344 Section 3.1 paragraph 1). The primary digital bitstream is available at respective ones of said separate parties (Fig. 3). A selector selects n bits of the ciphertext generated for the encryption of the plaintext (page 344 Section 3.1 paragraph 1).

However Jung discloses selecting n bits of the ciphertext for a key stream, but Jung does not expressly disclose the bit stream being randomly selected and the selector being operable to use said random bit source to randomize said selection operation in an identical manner; and a copy of a part of a primary digital bit stream, said primary digital stream being located externally to the at least two separate parties.

Maurer discloses a secure digital transmission system wherein the keys is selected according to a predetermined algorithm (abstract). A copy of a part of a primary digital bit

stream (Fig. 1 part 21), said primary digital stream being located externally to the at least two separate parties, said copy being available at respective ones of said separate parties (Figure 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the externally located data stream of Maurer to distribute keys in the system of Jung. One of ordinary skill in the art would have been motivated to do this because it would allow for a more secure transmission system in which access to both key index and encrypted message does not enable access to future operational keys (Maurer column 2 lines 60-65).

Maurer does not disclose a selector for randomly selecting said parts of said primary digital bitstream.

Shefi discloses a comprising a selector for randomly selecting parts of a random number table to form a random source (column 11 lines 48-54). The random number is then used as part of the pointer or one-time key to find the next random number from the table and therefor the selector (pointer, one-time key) is operable to use the random bit source to randomize the selection operation in an identical manner (column 13 lines 16-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the method of random selection as in Shefi to select a key from the bit stream stored in the memory of Maurer. One of ordinary skill in the art would have been motivated to do this because the one time pad is theoretically unbreakable (column 3 lines 19-21), however both parties require the same random number generator that provides at least one identical pseudorandom number (column 5 lines 11-16).

In reference to claims 2, 15, and 22, wherein said primary bit stream is obtainable as a stream of bits from a data exchange process between said two parties (Fig. 3).

In reference to claims 3 and 23-24, wherein said bits in said primary bit stream are separately identifiable by an address, and wherein said selector is operable to select said bits by random selection of addresses. Jung discloses a shift register wherein the ciphertext is sent to; therefore an address that is identifiable and the register is used to store selected bitsream therefore selection of bits content (Fig. 3).

In reference to claims 4 and 25, wherein each selector comprises an address generator and each address generator is identically set.

Jung does not disclose a system wherein each selector comprises an address generator.

Shefi discloses a selector that creates a random number that is used as the pointer; the pointer is used to indicate the position of the real random number from the table of random numbers. Both parties as a result of having the same value for the pointer and the values in the table, has identical values for the generated random number (column 11 lines 48-55).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the method of selection of the random source as in Shefi in the system of Jung. One of ordinary skill in the art would have been motivated to do this because the one time pad is theoretically unbreakable (column 3 lines 19-21), however both parties require the same random number generator that provides at least one identical pseudorandom number (column 5 lines 11-16) and a practically unlimited number of electronic one-time pads (column 10 lines 15-20).

In reference to claim 5, wherein each address generator is operable to make use of a random bit stream to randomize said addresses generation.

Jung does not disclose a system wherein each address generator is operable to make use of a random bit stream to randomize said addresses generation.

Shefi discloses a system wherein the generated number that includes the selected random number and merged with the generated number which is then used as a pointer into the random number table (column 13 lines 16-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the method of selection of the random source as in Shefi in the system of Jung. One of ordinary skill in the art would have been motivated to do this because the one time pad is theoretically unbreakable (column 3 lines 19-21), however both parties require the same random number generator that provides at least one identical pseudorandom number (column 5 lines 11-16) and a practically unlimited number of electronic one-time pads (column 10 lines 15-20).

In reference to claims 6 and 26, further comprising a controller for exchanging control data between said parties to enable each party to determine that each selector is operating synchronously at each party (column 1 lines 52-51). The parties have a timing signal that is used to ensure that synchronously sampled signal.

In reference to claims 7-8,16, and 27, wherein said control data includes any one of a group comprising: redundancy check data of at least some of the bits from said random bit source, and a hash encoding result of at least some of the bits from said random bit source.

Jung does not disclose a system wherein said control data includes any one of a group comprising: redundancy check data of at least some of the bits from said random bit source, and a hash encoding result of at least some of the bits from said random bit source.

Shefi discloses a system wherein an identifier used to determine whether the device has the correct table of random numbers and therefore synchronize the two parties. The system uses a mathematical function that reversible, this includes a hash function, to generate the identifier (column 19 lines 60-65). The mathematical function uses the results of the one-time pad and therefore the random bit source. The random bit source is found using the pointer (address), therefore the pointer is used to come to the encryption of the identifier.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the reversible mathematical function to create an identifier for synchronization between the communicating parties as in Shefi in the system of Jung. One of ordinary skill in the art would have been motivated to do this because a system that does not have the correct tables and values will not be able to communicate with the processor, therefore the communicating devices will know that they have the same data and that the random number generators are creating the same pointers.

Claims 9-12, 17-20, 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jung, Shefi, Maurer as applied to claim 6 above, and further in view of Midgley et al. (6,460,055 B1).

In reference to claims 9,17-18, and 28-29, wherein the selector further comprises a resynchronizer operable to determine from said control data that synchronization has been lost between the parties and to regain synchronization based on a predetermined earlier part of the output of said random bit source.

Although Shefi discloses the determination that synchronization has been lost using the identifier as discussed in the rejection for claim 7, neither Shefi nor Jung disclose regaining synchronization based on a predetermined earlier part of the output.

Midgley discloses determining lost synchronization by detecting when a user changes files (column 7 lines 49-51). The system regains synchronization based on the journal files to update the target files (column 12 line 63 to column 13 line 12). Therefore the earlier part of the output (journal) is used to regain synchronization.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to regain synchronization using the method of Midgley in the system of Jung. One of ordinary skill in the art would have been motivated to do this because it would ensure that the target is updated in a transactionally safe way (Midgley column 13 lines 5-10).

In reference to claims 10, 19, and 30, further comprising a backup data exchanger for exchanging the data for regaining synchronization.

Jung and Shefi do not disclose a backup exchanger for exchanging the data for regaining synchronization.

Midgley discloses keeping a backup of the data exchange at the back up server (column 13 lines 13-25).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to keep a backup for synchronization using the method of Midgley in the system of Jung. One of ordinary skill in the art would have been motivated to do this because it would ensure that the target is updated in a transactionally safe way (Midgley column 13 lines 5-10).

In reference to claim 11, wherein the resynchronizer further comprises a backup data storage for storing previously exchanged data for regaining synchronization to be used for resynchronization with a party that has not made said exchange.

Jung and Shefi do not disclose the resynchronizer further comprises a backup data storage for storing previously exchanged data for regaining synchronization to be used for resynchronization with a party that has not made said exchange.

Midgley discloses keeping a backup of the data exchange at the back up server (column 13 lines 13-25).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to keep a backup for synchronization using the method of Midgley in the system of Jung. One of ordinary skill in the art would have been motivated to do this because it would ensure that the target is updated in a transactionally safe way (Midgley column 13 lines 5-10).

In reference to claims 12, 20, and 31, wherein said resynchronizer is operable to create in advance future data to be used for resynchronization for resynchronizing with a party that has made said exchange in advance.

Although Jung discloses the continuous generation of pseudo-random noise signal (column 3 lines 37-42), and therefore creation of advance future data, Jung does not disclose the resynchronization with a party.

Midgley discloses keeping a backup of the data exchange at the back up server (column 13 lines 13-25), which is used for resynchronization.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to keep a backup for synchronization using the method of Midgley in the system

of Jung. One of ordinary skill in the art would have been motivated to do this because it would ensure that the target is updated in a transactionally safe way (Midgley column 13 lines 5-10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, November 27, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100